ABSTRACT OF THE INVENTION

A secure processor is operable in normal and preferred modes, and includes a security kernel instantiated when the processor enters into preferred mode and a security key accessible by the security kernel during preferred mode. The security kernel employs the accessed security key to authenticate a secure application, and allows the processor to be trusted to keep hidden a secret of the application. To instantiate the application, the processor enters preferred mode where the security key is accessible, and instantiates and runs the security kernel. The security kernel accesses the security key and applies same to decrypt a key for the application, stores the decrypted key in a location where the application will expect same, and instantiates the application. The processor then enters the normal mode, where the security key is not accessible.